LEGISLATIVE AUDIT DIVISION

Scott A. Seacat, Legislative Auditor
John W. Northey, Legal Counsel

Deputy Legislative Auditors:
Jim Pellegrini, Performance Audit
Tori Hunthausen, IS Audit & Operations
James Gillett, Financial-Compliance Audit

May 2002

TO: Legislative Audit Committee Members

FROM: Tori Hunthausen, Deputy Legislative Auditor, Information Systems (IS) Audits

DATE: May 2002

RE: IS Audit: University of Montana Banner System (02DP-05)

INTRODUCTION

As part of the Legislative Audit Division audits of The University of Montana (UM), we conducted a limited scope information systems audit focusing on selected UM Banner Human Resource (HR), Finance, and Student Financial Aid processes. Included in the audit scope were objectives to establish the existence and confirm the operation of internal controls over the selected UM Banner processes, and determine the status of prior audit recommendations. We conducted the audit according to generally accepted government auditing standards. We will not formally report the internal control weaknesses we identified or the associated details as a cautionary measure. However, these details have been communicated in a management letter with a recommendation to establish a UM Banner access and security plan.

Overall we concluded that UM Banner system applications operate in a controlled environment for the selected process that were tested, with the exception of weaknesses identified over user access.

BACKGROUND

Banner is a delivered software product licensed to UM by Systems and Computer Technology Corporation. The University of Montana – Missoula and the UM campuses at Dillon, Butte, and Helena process their student information, financial aid, human resource, and financial data using Banner software applications. UM Banner Finance and Human Resources are operated and maintained centrally by UM Missoula Business Services and UM Computing & Information Services for all UM campuses. The UM Banner system operates in a client/server environment using an Oracle 8i object / relational database and a DEC VMS operating system.

AUDIT HISTORY

We perform audit procedures on selected UM Banner processes approximately every two years. The prior UM Banner Information Systems audit reported four issues. Of these four issues, three recommendations were implemented by UM management and one issue is partially implemented.

Room 160, State Capitol Building PO Box 201705 Helena, MT 59620-1705
Phone (406) 444-3122 FAX (406) 444-9784 E-Mail lad@state.mt.us

CURRENT STATUS OF PRIOR AUDIT RECOMMENDATION

We included UM Banner user access in our current audit scope as a follow-up procedure to a prior audit recommendation (00DP-09 Recommendation #1 Access to Critical Banner Forms) and because security and access controls are a significant element of the UM Banner environment. We acknowledge UM management's commitment to strong internal controls and the efforts staff have made to improve access controls and correct the previously existing system condition. However, based on the results of our testing, we believe it necessary to conclude the prior audit recommendation is partially implemented and to revisit the issue.

Our testing indicates that two conditions continue to exist: One, current procedures do not prevent individuals whose need has expired, students not currently working with a program, or terminated employees from accessing UM data. Two, current procedures do not lessen the potential for unauthorized HR transactions. We attribute these conditions to the lack of a single, comprehensive, written UM Banner security plan for the following reasons.

Inherent to the operation of automated systems and information use is the concept of deciding who has access to the system and access to information contained in the system. Information industry control objectives state that management is responsible for planning, developing, and implementing a control structure to provide a secure computing environment. According to information industry best practices and guidance, the control structure is documented in the form of a written plan. Internal controls can then be implemented by following plan contents. The plan is not static but a foundation of a security cycle that continually operates and requires that staff identify critical system and application functions, assess risks to the system, monitor security procedures and adjust procedures to maintain plan effectiveness. UM Banner could benefit from a comprehensive written security plan that applies to all Banner modules, business process owners, and UM campuses.

It is our opinion that such a plan would be beneficial to the university. The benefits of developing a written and comprehensive security/access plan are:

- to identify and mitigate risks to UM Banner operations,
- to create system controls or compensating controls for identified risks,
- to provide staff with a uniform and shared understanding of required security procedures that is necessary for:
    - consistent application in a decentralized multi-campus environment,
    - proper implementation of controls,
    - clear understanding of both user and administrator responsibilities,
    - and elements to monitor for determining control effectiveness,
- to demonstrate that management has developed a structure to minimize the opportunity for unauthorized access to information which may result in misuse, unauthorized disclosure, damage, or loss of data.

We discussed this concern with UM management, as required by generally accepted government auditing standards, and presented the following recommendation to address the condition:

RECOMMENDATION

We recommend UM personnel develop a written UM Banner Application access and security plan.